Listing of the Claims:

The listing of claims below will replace all prior versions and listings of claims in this Application.

1. (Previously Presented) An apparatus comprising:

a tamper resistant digital content recovery module to recover protected digital contents of various types, the recovery module employing measures to hinder observation of operations performed therein;

a plurality of plain text digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules, with selective combinations of the plain text digital content rendering modules to be selectively employed to render the recovered digital contents of the various types, including one of the plain text digital content rendering modules occupying a root position of the hierarchy to exclusively receive all types of the recovered digital contents to be rendered, from the tamper resistant digital content recovery module;

one or more storage units operative to store said tamper resistant module and said plurality of plain text digital content rendering modules; and

a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules.

2. (Previously Presented) The apparatus of claim 1, wherein the tamper resistant digital content recovery module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy as not having been compromised, and to provide recovered digital content to the plain text digital content rendering module occupying the root position of the hierarchy, only upon having verified the plain text digital content rendering module occupying the root position of the hierarchy as not having been compromised.

3. (Previously Presented) The apparatus of claim 2, wherein the tamper resistant digital content recovery module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy, responsive to a request from the plain text

digital content rendering module occupying the root position of the hierarchy to recover a protected digital content.

4. (Previously Presented) The apparatus of claim 3, wherein the tamper resistant digital content recovery module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy by verifying a signature of the plain text digital content rendering module occupying the root position.

5. (Previously Presented) The apparatus of claim 1, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised.

6. (Previously Presented) The apparatus of claim 5, wherein the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised, at least during initialization.

7. (Previously Presented) The apparatus of claim 6, wherein the non-leaf modules is equipped to further verify the immediate downstream module remains un-compromised before each transfer of recovered digital content to the immediate downstream module.

8. (Previously Presented) The apparatus of claim 5, wherein the a non-leaf modules is equipped to verify the immediate downstream module as not having been compromised by verifying a signature of the immediate downstream module.

9. (Previously Presented) The apparatus of claim 1, wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types.

10. (Previously Presented) The apparatus of claim 1, wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, or a cluster of coupled systems.

11. (Original) The apparatus of claim 1, wherein a first subset of the plain text digital content rendering modules are member modules of a first application domain, and a second subset of the plain text digital content rendering modules are member modules of a second application domain.

12. (Previously Presented) A processor implemented method, comprising:

a root one of a plurality of hierarchically organized plain text digital content rendering modules collectively adapted to render digital contents of a plurality of types;

requesting a tamper resistant digital content recovery module to recover a first protected digital content of a first type;

verifying with the tamper resistant digital content recovery module that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been compromised;

recovering with the tamper resistant digital content recovery module the first protected digital content in an obfuscated manner;

transferring the recovered first digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules;

rendering with said root one in conjunction with first at least one other one of said plurality of hierarchically organized plain text digital content rendering modules said first digital content; and

verifying with said root one of the modules that one of the first at least one other one of the modules occupying an immediate downstream position in the hierarchy of modules from the root module, is uncompromised before transferring the first digital content to the verified immediate downstream module to further the rendering of the first digital content.

13. (Previously Presented) The method of claim 12, wherein the tamper resistant module verifies the root one of the plurality of hierarchically organized plain text digital content rendering modules by verifying the root one's signature.

14. (Previously Presented) The method of claim 12, wherein said root one verifies the one of the first one other one that occupies an immediate downstream position in the hierarchy of

modules from the root module is uncompromised by verifying the immediate downstream module's signature.

15. (Previously Presented) The method of claim 12, wherein the method further comprises said root one verifies each module occupying an immediate downstream position in the hierarchy of modules from the root modules during initialization.

16. (Previously Presented) The method of claim 12, wherein the method further comprises:

the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of the same first type;

the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been compromised;

the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with said root one re-verifying the same immediate downstream module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

17. (Previously Presented) The method of claim 12, wherein the method further comprises:

the root one of the plurality of hierarchically organized plain text digital content rendering modules requesting the tamper resistant digital content recovery module to recover a second protected digital content of a second type;

the tamper resistant digital content recovery module verifying that said root one of the plurality of hierarchically organized plain text digital content rendering modules has not been compromised;

the tamper resistant digital content recovery module recovering the second protected digital content in an obfuscated manner, and transferring the recovered second digital content to said root one of the plurality of hierarchically organized plain text digital content rendering modules; and

said root one in conjunction with second at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with said root one verifying one of the second at least one other one occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content.

18. (Previously Presented) An apparatus comprising:

a plurality of digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules, with selective combinations of the modules to be selectively employed to protectively render digital content of various types, including one of said digital content rendering modules occupying a root position of the hierarchy to exclusively receive the various types of digital contents to be rendered, from a recovery module not part of the hierarchy of modules, the recovery module being responsible for recovering the digital contents from their ciphered states, the recovery module employing measures to hinder observation of operations performed therein, and the root modules being operative for verifying a module occupying an immediate downstream position in the hierarchy of modules from the root module as not having been compromised;

one or more storage units to store said plurality of digital content rendering modules; and a processor coupled with the one or more storage units to execute the digital content rendering modules.

19. (Previously Presented) The apparatus of claim 18, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised, at least during initialization.

20. (Previously Presented) The apparatus of claim 18, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and the non-leaf modules is equipped to further verify to the immediate downstream module remains uncompromised before each transfer of digital contents to the immediate downstream digital content rendering module.

21. (Previously Presented) The apparatus of claim 20, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised, by verifying a signature of the immediate downstream modules.

22. (Previously Presented) The apparatus of claim 18, wherein the digital content of various types comprises streaming media contents of a plurality of media types, and of a plurality of format types.

23. (Previously Presented) The apparatus of claim 18, wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, or a cluster of coupled systems.

24. (Previously Presented) The apparatus of claim 18, wherein a first subset of the modules are member modules of a first application domain, and a second subset of the modules are member modules of a second application domain.

25. (Previously Presented) A processor implemented method comprising;

verifying with a root one of a plurality of hierarchically organized digital content rendering modules, that each module that occupies an immediate downstream position in the hierarchy of modules from the root module has not been compromised, during an initialization period;

exclusively receiving with the root one of the plurality of hierarchically organized digital content rendering modules a first digital content of a first type;

rendering in part with said root one of said modules said first digital content;

re-verifying with said root one of said modules that one of the at least one other one of the modules occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised; and

transferring with said root one of said modules the first digital content to the re-verified immediate downstream module to further the rendering of the first digital content.

26. (Previously Presented) The method of claim 25, wherein said root one verifies each immediate downstream module is uncompromised by verifying the immediate downstream module's signature.

27. (Previously Presented) The method of claim 25, wherein the method further comprises:

the root one of the plurality of hierarchically organized plain text digital content rendering modules receiving a second protected digital content of the same first type; and

said root one in conjunction with the same first at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with said root ones re-verifying the same one of the first at least one other one that occupies an immediate downstream position in the hierarchy of modules from the root module is uncompromised before transferring the second digital content to the immediate downstream module to further the rendering of the second digital content

28. (Previously Presented) The method of claim 25, wherein the method further comprises:

the root one of the plurality of hierarchically organized plain text digital content rendering modules receiving a second protected digital content of a second type; and

said root one in conjunction with second at least one other one of said plurality of hierarchically organized digital content rendering modules rendering said second digital content, with said root one re-verifying one of the second at least one other one occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised before transferring the second digital content to the re-verified one of the second at least one other one occupying an immediate downstream position in the hierarchy of modules from the root module to further the rendering of the second digital content.

29. (Previously Presented) An article of manufacture comprising:

a recordable medium;

a first plurality of programming instructions recorded on said recordable medium, said first programming instructions adapted to program a computing device to implement on the computing device a tamper resistant digital content recovery module to recover protected digital contents of various types , the recovery module employing measures to hinder observation of operations performed therein; and

a second plurality of programming instructions recorded on said recordable medium, said second programming instructions operative to program a computing device to implement on the computing device a plurality of plain text digital content rendering modules, said rendering modules communicatively coupled with each other in a hierarchical manner to form a hierarchy of modules the plain text digital content rendering modules being selectively employed in combination to render the recovered digital contents of the various types including one of the plain text digital content rendering modules occupying a root position of the hierarchy to exclusively receive all types of the recovered digital contents to be rendered from the tamper resistant digital content recovery module.

30. (Previously Presented) The article of claim 29, wherein the tamper resistant digital content recovery module is equipped to verify the plain text digital content rendering module occupying the root position of the hierarchy has not been compromised, and to provide recovered digital content to the plain text digital content rendering module occupying the root position of the hierarchy, only upon having so verified that the plain text digital content rendering module occupying the root position of the hierarchy has not been compromised.

31. (Previously Presented) The article of claim 29, wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module and the non- leaf module is equipped to verify the immediate downstream module from the non-leaf module as not having been compromised.

32. (Previously Presented) The article of claim 29, wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types.

33. (Original) The article of claim 29, wherein the recordable medium is a selected one of a magnetically recordable medium and an optically recordable medium.

34. (Withdrawn) A method comprising:

with a tamper resistant digital content recovery module, recovering a first protected digital content of a first type in an obfuscated manner;

with said tamper resistant digital content recovery module, verifying that a root module of a plurality of hierarchically organized plain text digital content rendering modules has not been compromised;

with said root module, verifying that at least one other module of said plurality of hierarchically organized plain text digital content rendering modules has not been compromised, wherein the at least one other module occupies an immediate downstream position in the hierarchy of modules from said root module; and

rendering with said root module and at least said one other module said first digital content.

35. (Withdrawn) The method of claim 34, wherein verifying that a root module of a plurality of hierarchically organized plain text digital content rendering modules has not been compromised comprises verifying a signature of said root module.

36. (Withdrawn) The method of claim 34, wherein verifying that at least one other module of said plurality of hierarchically organized plain text digital content rendering modules has not been compromised comprises verifying a signature of said one other module.

37. (Withdrawn) The method of claim 34, and further comprising:

with said root module, verifying that a plurality of other modules occupying an immediate downstream position in the hierarchy of modules from said root module have not been compromised during an initialization.

38. (Withdrawn) An apparatus comprising:

a plurality of digital content rendering modules organized in a hierarchical manner;

a root module of said plurality of digital content rendering modules operable to verify that an immediate downstream module in the hierarchy of said plurality of digital content rendering modules has not been compromised;

a tamper resistant content recovery module operable to recover digital content of various types from a ciphered state in an obfuscated manner, and further operable to verify that said root module has not been compromised; and

wherein said root module along with at least said immediate downstream module are operable to render a plain text version of the recovered digital content.

39. (Withdrawn) The apparatus of claim 38, and further comprising a non-leaf module occupying a non-leaf position in the hierarchy, wherein said non-leaf module is operable to verify that a module occupying a downstream position of the non-leaf module in said hierarchy has not been compromised, at least during initialization.

40. (Withdrawn) The apparatus of claim 38, and further comprising a non-leaf module occupying a non-leaf position in the hierarchy, wherein said non-leaf module is operable to verify that a module occupying a downstream position of the non-leaf module in said hierarchy has not been compromised before each transfer of the recovered digital content to said module occupying a downstream position.

41. (Withdrawn) The apparatus of claim 38, and further comprising and further comprising a non-leaf module occupying a non-leaf position in the hierarchy, wherein said non-leaf module is operable to verify that a module occupying a downstream position of the non-leaf module in said hierarchy has not been compromised by a verifying a signature of said module occupying a downstream position.

42. (Withdrawn) The apparatus of claim 38, wherein said digital content of various types comprises streaming media contents of a plurality of media types, and of a plurality of format types.